DMS/Medium Grade Services Interim External Certificate Authority

Meeting of the Minds

Betsy Appleby
APPLEBYB@NCR.DISA.MIL
(703) 681-0283
7 March 00

Why We Are Here Today

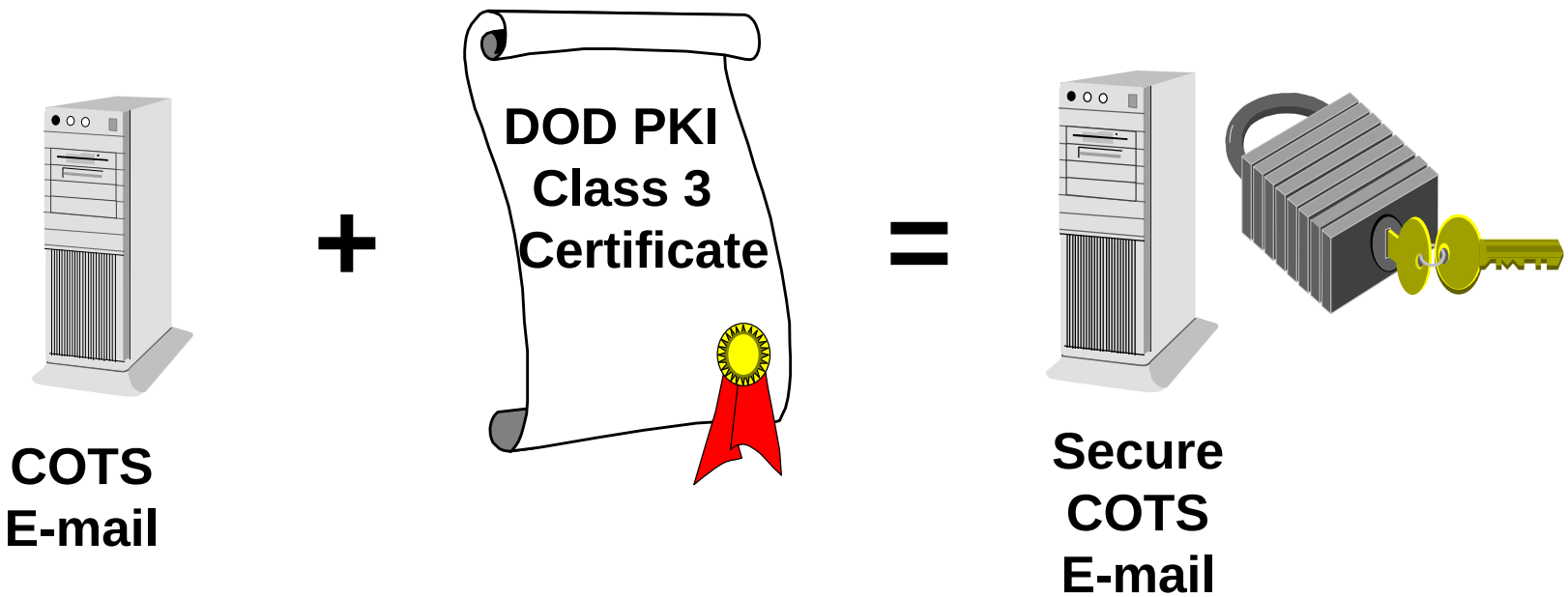
- **To share DOD objectives for secure email capability**
- **To discuss role of IECAs in achieving this objective with DOD contractors/vendors**
- **To describe USMC Medium Grade Services implementation plan**
- **To give assessment of current IECA process from end-user perspective**

What is DMS/MGS?

DMS/MGS is secure interoperable commercial off-the-shelf (COTS) email that uses the DOD Public Key Infrastructure (PKI) Medium Assurance certificates for signature and encryption

DMS/MGS
PKI and MGS

In MGS, the DoD PKI provides an e-mail certificate that is bound to the user's e-mail address and enables the user to send and receive signed and encrypted e-mail to and from other MGS users.

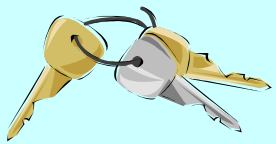


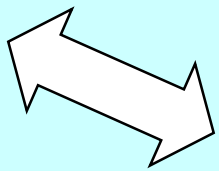
MGS Ground Rules

- **MGS = COTS**
- **MGS will use DOD PKI Medium Assurance Certificates for Signature and Encryption**
- **Trust BUT Verify testing approach**
  - **Multi-vendor product interoperability**
  - **DOD PKI readiness**
- **Gain early operational experience through pilots**

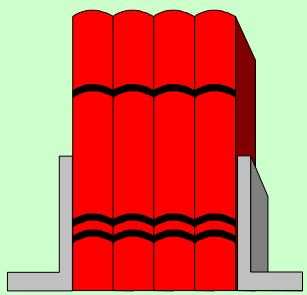
MGS Activities

DoD PKI





1. Lab Integration

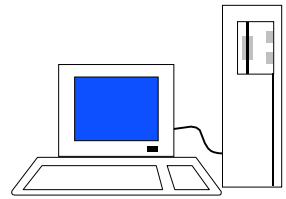


2. Create User Documentation

5th Signal

3. Pilot Rollout

Lab Activities
Completed



1. Installed and Configured

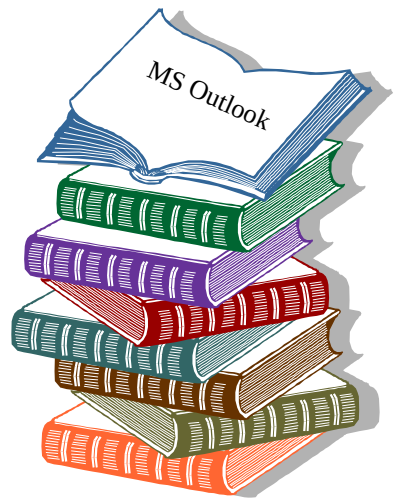
- Clients (on Windows 95, 98, NT)
  - MS Outlook ‘98
  - MS Outlook Express 5
  - Netscape Communicator 4.7
  - Lotus Notes 5.01a
- Servers:
  - MS Exchange 5.5 SP2
  - Lotus Notes 5.01a

2. Executed Comprehensive Interoperability Test Suite

- Signed
- Encrypted
- Signed and Encrypted

MGS Products Verified for Interoperability

- **Generated Step-By-Step User's Guides for the Retrieval of DOD PKI Certificates and Configuration of E-mail Clients**
  - **Lotus Notes 5.01a**
  - **Microsoft Outlook Express 5.0**
  - **Microsoft Outlook 98/2000**
  - **Netscape Communicator 4.7**



Background Policy
Driving the MGS High Demand

Deputy Secretary of Defense Memorandum, 6 May 1999, Department of Defense (DoD) Public Key Infrastructure (PKI)

- **All DoD Users will, at a minimum, be issued a Class 3 certificate by October 2001**
- **All electronic mail (as distinct from organizational messaging) sent within the Department will be signed using appropriate protocols consistent with the Department's email strategy by October 2001**
- **Department of Defense components are encouraged to encrypt email within the Department**

MGS Pilot Criteria

- **Each pilot brings unique scenarios**
  - **USAREUR - Replace PGP - ‘Train the Trainer’ - Roving kiosks for registration**
  - **USMC - IECAs - USMC Email Policy**
  - **USAF - Registration using ‘trusted agents’**
- **Pilot partner must document and disseminate lessons learned**
- **MGS Pilot solutions MUST be scalable**

Definition: IECA

- **Interim External Certification Authorities (IECAs)**
  - **Certification Authorities that provided non-DOD personnel with certificate services that are interoperable with the DOD PKI**
  - **Operated by organizations other than the DOD**
  - **IECA certificates not signed by the DOD Root; hence DOD applications use IECAs as trust anchors**
  - **Short-Term Solution for DOD**

IECA Vendors

- Operational Research Consultants (ORC)
- Digital Signature Trust (DST)
- VeriSign, Inc.
- General Dynamics

MGS/IECA Involvement

- **MGS Day w/IECAs – TODAY**
- **End-to-End Process Validation**
  - **Documented IECA Registration Process of USMC Contractors/Vendors**
- **Participate in DOD PKI Team Kick-Off Meetings w/IECA Vendors**
- **MGS Boosts Demand for IECAs**
  - **Integrating IECA into MGS General Procedures**

DOD Trading Partner PKI User Registration Process

Individual Contractor is Selected to do Business with DOD

Contractor Selects IECA of Choice
View IECAs at:

www.disa.mil:80/infosec/pkieca/iecas.html

Download IECA Trust Anchor (Root Certificate)

Begin Request for Email and/or ID Certificates (X.509)

Generate Key Pair

Print Form and Notarize

Send Notarized From to IECA for Approval

3-5 Days

Receive Approval with Access Codes and Instructions

Obtain Certificate (X.509v3) from IECA

Enable Email and Browser for PKI

IECA Suggestions
Ease of Use

- **Keep User Friendly**
  - **Confusing Web Site**
  - **Terminology**
- **Post Bulk Pricing**
- **On-site Registration Quick Guides for Contractors**
  - **Certificate Retrieval**
  - **Certificate Verification (CRL's)?**
- **Post Common Terminology**

Recommended IECA Common Terminology

Identity Certificate - This is a digital certificate associated with the end entities' digital signature which will be used where non-repudiation is required meaning the end entity cannot deny responsibility for any execution of authenticated transactions. The intent is that the use of this digital signature certificate legally binds the end entity to that transaction.

- **Some examples for its uses might include:**
- **document signing**
- **claims signing**
- **secure web access (note however that this does not require nonrepudiation)**

Note: “digitalSignature” and “nonRepudiation” bit are asserted. See RFC 2459 for details.

IECA Common Terminology Con't

Encryption Certificate - This digital certificate is used where encryption and/or digital signatures are required. It is used for execution of transactions where non-repudiation is not required.

Some examples for its uses include:

- **email messaging**
- **secure web access**
- **document encrypting**

Note: "digitalSignature" and "keyEncipherment" bits are asserted. See RFC 2459 for details at http://www.ietf.org

IECA REGISTRATION COMPARISON

	DST https://secure.digsigtrust.com/ieca/	GD http://gd.cs.com/ieca	ORC http://eca.orc.com/index2.html	VeriSign http://www.verisign.com/gov/ieca/
Supported Browsers (FIPS 140-1)	**Netscape 4.05 > (Domestic)**		**Netscape 4.05> (Domestic)**	**Netscape 4.05 > IE 5.01 > (Domestic)**
Certificate Pricing / year	**ID - $250 Email - $250 Both - $475**		**ID - $ N/A Email - $ N/A Both - $250**	**ID - $195 Email - $195 Both - $295**
Identity Validation	**Face-to-Face or Notary (applying organization or Finacial institution only) with: - 1 Government Photo ID**		**Face-to-Face or Notary (any) with: - Drivers License**	**Face-to-Face or Notary (any) with: -1 Government Photo ID -2 Other ID**
Key Generation	**At time of Registration**		**At time of Registration**	**Upon Approval via email**
Approval Notification	**U.S. Mail**		**Email**	**Email**
Turn Around Time	**13 days (Notary Denied, I didn't follow directions and approval via U.S mail)**		**5 days**	**4 days**

How to *Operationalize* MGS

- **Establish Technical Environment**
  - RA/LRA Technical Infrastructure(people/HW/SW)
  - Email product & Internet browsers meet minimal requirements
  - Support staff and core users are postured for MGS
- **Define Process/Publish Procedures**
  - Outline the process of registering and enabling email
  - Provide step-by-step procedures
  - Identify MGS cadre to capture lessons learned

How to *Operationalize* MGS (cont.)

- ***Train the Trainers*** **with classroom & hands-on instruction**
  - **Register and train support staff and power users**
  - **Train Help Desk**
  - **Train initial core group in using MGS in daily activities**
- **Follow-up -** ***Building on Success***
  - **Provide third-tier support**
  - **Collaborate with COTS email vendors to solve systematic problems**
  - **Provide Updates/Enhancements to MGS User Base**

COTS Facts of Life

- **New product releases and versions occur frequently**
- **COTS versions generally newer than fielded DMS User Agents**
- **Configuration is Everything!**
  - **A wide variety of configurations will work for basic SMTP**
  - **Only a few configurations will work for MGS**
  - **Pilot sites often have heterogeneous configurations installed**

MGS Bottom Line

- **MGS is PKI Ready and being used today**
  - ***PKI Ready* is Changing**
- **Email crosses all boundaries and is on every desktop**
- **The time is right for MGS implementation**
- **Continue work with vendors, develop tools, test products & processes, and manage knowledge for the benefit of all DOD users**

MGS is not a *product* - it is a *capability*

MGS/IECA Way Ahead

- **Build MGS Partnership with IECA Vendors**
  - **'7-Day' Forecast for DOD Contractor/Vendor IECA Demand**
  - **Share COTS Email Application issues**
  - **Streamline MGS implementation (internal/external)**

- **Adhere to best commercial practices - we need your HELP!**

Back-Up Charts

MGS/PKI Problem Space